Asistente para la evaluación de características de calidad de producto de software propuestas por ISO/IEC 25010 basado en métricas definidas usando el enfoque GQM

Julieta Calabrese, Rocío Muñoz, Ariel Pasini, Silvia Esponda, Marcos Boracchia, Patricia Pesado

Instituto de Investigación en Informática LIDI (III-LIDI)*
Facultad de Informática – Universidad Nacional de La Plata
50 y 120 La Plata Buenos Aires
*Centro Asociado Comisión de Investigaciones Científicas de la Pcia. de Bs. As. (CIC)
{jcalabrese,rmunoz,apasini,sesponda,marcosb,ppesado}@lidi.info.unlp.edu.ar

Abstract. Se presenta un asistente para evaluar las características de un producto de software, propuestas por la ISO/IEC 25010 mediante el enfoque GQM (Goal, Question, Metric). Se definieron un conjunto de preguntas cuyas respuestas combinadas de forma lógica permiten obtener una métrica aplicable a las características que propone ISO/IEC 25010. Para este trabajo se tomó como caso de estudio la característica de Seguridad, se definieron las métricas y luego se muestran los resultados de la aplicación a tres casos de estudio.

Keywords: Calidad, Producto de software, GQM, ISO/IEC 25000

1 Introducción

El número de empresas desarrolladoras de software ha experimentado un fuerte crecimiento, juntamente con el incremento de la demanda de productos del sector. Para este tipo de empresas, la calidad del software tiene un papel fundamental, en particular como elemento diferenciador de competitividad y de imagen frente a sus clientes y porque consecuentemente, las pérdidas económicas que los problemas de la calidad en el software pueden ocasionar son considerables. En este contexto, las actividades relacionadas con la calidad de software y su evaluación, están cobrando cada vez más importancia. [1]

Una organización puede interesarse en evaluar su producto pues desea diferenciarse de los competidores, asegurando tiempos de entrega y reducción de fallos en el producto tras su implantación en producción; establecer acuerdos en el ámbito del servicio, definiendo parámetros de calidad que el producto debe cumplir antes de ser entregado; detectar los defectos en el producto software y proceder a su eliminación antes de la entrega; evaluar y controlar el rendimiento del producto software desarrollado, asegurando que podrá generar los resultados teniendo en cuenta las restricciones de tiempo y recursos establecidas; asegurar que el producto software

desarrollado respeta los niveles necesarios para las características de seguridad (*Confidencialidad*, *Integridad*, *Autenticidad*, *No-Repudio*, etc.) entre otras.
En este sentido, la familia ISO 25000 conocida como SQuaRE (Software Product Quality Requirements and Evaluation) nace para dar respuesta a estas necesidades. Su objetivo es la creación de un marco de trabajo común para evaluar la calidad del producto software, sustituyendo a las anteriores ISO/IEC 9126 e ISO/IEC 14598 Modelos de calidad y generación de métricas. [2]–[4]
En el presente trabajo se propone un asistente de evaluación de productos de software basado en las métricas definidas en ISO/IEC 25010 usando el enfoque GQM. [5]
En la sección 2 se describe brevemente la familia de la ISO/IEC 25000 y el enfoque que propone GQM. A continuación, apartado 3, se describe el modelo para realizar la evaluación de las características propuestas por ISO/IEC 25010 bajo el enfoque GQM, en particular de la característica de ***Seguridad***. Luego se presentan tres casos de estudio, donde se aplica el modelo de evaluación junto con los resultados obtenidos de las mismas. Por último, las conclusiones del presente trabajo.

2 Modelos de calidad y generación de métricas

2.1 La familia de ISO/IEC 25000.

La gestión de la calidad se impone en las organizaciones por la importancia que alcanza en diferentes aristas: a nivel de sus productos, permitiendo establecer la calidad lograda y las características presentes en los mismos; a nivel de la organización, ocupándose de establecer un marco de procesos que permita obtener una mejora; como asimismo a nivel de proceso.

Con el objetivo de organizar y unir todas las normas relacionadas con la calidad de los productos de software, en el año 2005 ISO/IEC publica ISO/IEC 25000:2005 - SQuaRE (Requisitos y evaluación de la calidad del producto de software), también conocida como la familia ISO 25000. Dentro del conjunto del ISO/IEC 25000, se destacan ISO/IEC 25010 - *System and software quality models* e ISO/IEC 25040 - *Evaluation process* que se describen a continuación.

ISO/IEC 25010 - System and software quality models.
Reemplaza a la ISO/IEC 9126-1:2001. Incorpora nuevas características internas y externas, agrupándolas bajo el nombre de calidad del producto de software. La principal modificación es la incorporación de la característica ***Compatibilidad*** que se relaciona con la posibilidad de intercambio de información entre sistemas, y la característica ***Seguridad*** que se relaciona con los conceptos de confidencialidad y acceso a la información.[6]

Cada una de las características de la calidad del producto de software posee subcaracterísticas que las especifican más claramente según se muestra en la Figura 1.

Figura 1

ISO/IEC 25040 - Evaluation process.
Reemplaza a la ISO/IEC 14598-1:1999. La nueva versión define 13 procesos en cinco etapas:
1) Establecer los requisitos de la evaluación: a. Establecer el propósito de la evaluación. b. Obtener los requisitos de calidad del producto. c. Identificar las partes del producto que se deben evaluar. d. Definir el rigor de la evaluación.
2) Especificar la evaluación: a. Seleccionar los módulos de evaluación. b. Definir los criterios de decisión para las métricas. c. Definir los criterios de decisión de la evaluación.
3) Diseñar la evaluación: a. Planificar las actividades de la evaluación.
4) Ejecutar la evaluación: a. Realizar las mediciones. b. Aplicar los criterios de decisión para las métricas. c. Aplicar los criterios de decisión de la evaluación.
5) Finalizar la evaluación: a. Revisar los resultados de la evaluación. b. Crear el informe de evaluación. c. Revisar la calidad de la evaluación y obtener feedback. d. Tratar los datos de la evaluación. [7]

2.2 GQM. (Goal, Question, Metric)

GQM (Goal, Question, Metric) es un método orientado a lograr una métrica que mida cierto objetivo de una manera determinada. El modelo de medición tiene tres niveles:

- Nivel Conceptual (Goal/Objetivo): se define un objetivo para un objeto, el cual puede ser un producto, un proceso o un recurso, con respecto a varios modelos de calidad, desde varios puntos de vista y relativo a un entorno particular.
- Nivel Operativo (Question/Pregunta): se refina un conjunto de preguntas a partir del objetivo, con el propósito de verificar su cumplimiento. Las preguntas tratan de caracterizar el objeto de medición (producto, proceso o recurso) con respecto a una cuestión de calidad seleccionada y determinar su calidad desde el punto de vista seleccionado.

- Nivel Cuantitativo (Metric/Métrica): se asocia un conjunto de métricas, que pueden ser objetivas o subjetivas, para cada pregunta, de modo de responder a cada una de un modo cuantitativo.

Un modelo GQM se desarrolla identificando un conjunto de objetivos de calidad y/o productividad, a nivel corporativo, de división o de proyecto. A partir de esos objetivos y en base a modelos del objeto de medición, se elaboran preguntas que definen esos objetivos de la manera más completa posible. El siguiente paso consiste en especificar las medidas que deben ser tomadas para responder a esas preguntas y para realizar un seguimiento de la conformidad de los productos y procesos con los objetivos. Una vez especificadas las medidas, es necesario desarrollar los mecanismos de recopilación de información, incluidos los mecanismos de validación y análisis. [5]

3 Modelo de Evaluación de características de Calidad

El modelo desarrollado consiste en definir un conjunto de preguntas basadas en el enfoque GQM que luego, mediante conectivos lógicos, indicarán la satisfacción de los objetivos propuestos.
Como caso de estudio se tomó la característica ***Seguridad*** que contiene las subcaracterísticas: *Confidencialidad*, *Integridad*, *No-Repudio*, *Responsabilidad* y *Autenticidad*.

CONFIDENCIALIDAD: Evalúa la capacidad de protección contra el acceso de datos e información no autorizados, ya sea accidental o deliberadamente.
INTEGRIDAD: Evalúa la capacidad del sistema o componente para prevenir accesos o modificaciones no autorizados a datos o programas de ordenador.
NO-REPUDIO: Evalúa la capacidad de demostrar las acciones o eventos que han tenido lugar, de manera que dichas acciones o eventos no puedan ser repudiados posteriormente.
RESPONSABILIDAD: Evalúa la capacidad de rastrear de forma inequívoca las acciones de una entidad.
AUTENTICIDAD: Evalúa la capacidad de demostrar la identidad de un sujeto o un recurso.

3.1 Cuestionario

En función de las subcaracterísticas descriptas anteriormente, se definieron 33 preguntas para responder con verdadero/falso. Tabla 1

Tabla 1. Cuestionario para la característica de ***Seguridad***

ID	PREGUNTA
P1	¿Se requiere que la contraseña posea al menos 8 caracteres?
P2	¿Se requiere que la contraseña posea letras mayúsculas y minúsculas?
P3	¿Se requiere que la contraseña posea números y letras?

P4	¿Se requiere que la contraseña posea caracteres especiales?
P5	¿El sistema utiliza conexión segura mediante HTTPS?
P6	¿La base de datos posee los datos encriptados?
P7	¿El sistema permite acceder a funcionalidades en las cuales no se tiene permiso?
P8	¿El sistema permite que cualquier persona tenga acceso a la base de datos?
P9	¿El sistema permite que cualquier persona tenga acceso al código del servidor de la aplicación?
P10	¿Cualquier persona tiene acceso al servidor físico?
P11	¿Cualquier persona tiene acceso al servidor remoto?
P12	¿El sistema posee redireccionamientos hacia sitios no seguros?
P13	¿El sistema solicita una confirmación de registro mediante un mail a la hora de registrarse?
P14	¿El sistema permite que cualquier persona pueda modificar la base de datos?
P15	¿El sistema permite que cualquier persona pueda modificar el código del servidor de la aplicación?
P16	¿El sistema permite inyecciones SQL?
P17	¿El sistema posee un historial de acciones realizadas?
P18	¿El sistema posee algoritmos de cifrado de datos?
P19	¿El sistema posee un mecanismo criptográfico, como firma digital?
P20	¿El sistema solicita confirmación a la hora de realizar una acción?
P21	¿El sistema posee una protección con certificados SSL?
P22	¿El sistema da aviso cuando se accede desde una ubicación desconocida?
P23	¿El sistema informa vía mail las operaciones realizadas?
P24	¿El sistema guarda un registro de fecha y hora de ingreso al mismo?
P25	¿El sistema registra el tipo de navegador y sistema de operación utilizado para ingresar al sitio?
P26	¿El sistema registra la dirección IP desde la cual se ingresa al sitio?
P27	¿El sistema realiza una comprobación de identidad mediante un certificado digital?
P28	¿El sistema posee un sistema de verificación en dos pasos?
P29	¿Es requerida una clave de segundo nivel para el ingreso al sistema?
P30	¿El sistema realiza una comprobación de identidad mediante datos biométricos?
P31	¿El sistema realiza una comprobación de identidad mediante tarjeta de coordenadas?
P32	¿El sistema realiza una comprobación de identidad mediante credenciales?
P33	¿El sistema realiza una comprobación de identidad mediante una firma electrónica?

3.2 Descripción de criterios de evaluación (CE)

Con el fin de lograr el objetivo, las respuestas de las preguntas fueron combinadas de forma lógica estableciendo un puntaje a cada uno de los CE.

Tabla 2. Descripción de criterios de evaluación (CE)

ID	*Nombre*	*Descripción*	*Fórmula*	*Ptos*
C-1	Conexiones seguras	Una conexión se considera segura si se utiliza HTTPS y si no se tienen redireccionamientos hacia sitios no seguros	P5 & ~P12 = V	1
C-2	Control de acceso	Se debe controlar que no se permita acceder a funcionalidades sin autorización, tampoco a la base de datos, al código de la aplicación ni a los servidores, físico ni remoto	si P7 | P8 | P9 | P10 | P11 = F	1
C-3	Encriptación de datos	Los datos de la base de datos deben estar encriptados	P6 = V	1
C-4	Contraseña de bajo nivel	La contraseña se considera de bajo nivel si posee menos de 8 caracteres, no posee letras mayúsculas y minúsculas, no posee letras y números y no posee caracteres especiales	P1 | P2 | P3 | P4 = F	0
	Contraseña de medio nivel	La contraseña se considera de medio nivel si posee al menos 8 caracteres o letras mayúsculas y minúsculas o letras y números o	P1 | P2 | P3 | P4 = V	0.5
	Contraseña de alto nivel	La contraseña se considera de alto nivel si posee al menos 8 caracteres, letras mayúsculas y minúsculas, letras y números y caracteres especiales	P1 & P2 & P3 & P4 = V	1
I-5	Prevención de accesos	Se debe prevenir que no se permita acceder a funcionalidades sin autorización, tampoco a la base de datos ni al código de la aplicación, y que no se permitan inyecciones SQL	P7 | P8 | P9 | P16 = F	1
I-6	Prevención de modificaciones	Se debe prevenir que no se permita modificar datos de la base de datos ni modificar el código de la aplicación sin autorización	P14 | P15 = F	1
I-7	Confirmación de datos	Se debe realizar una confirmación de registro por mail	P13 = V	1
NR-8	Operaciones realizadas	Se debe poseer un historial de acciones realizadas o las mismas deben ser enviadas por mail	P17 | P23 = V	1
NR-9	Mecanismos de cifrado	Se debe poseer un algoritmo de cifrado de datos o un mecanismo criptográfico, como firma digital, o una protección con certificados SSL	P18 | P19 | P21 = V	1
NR-10	Confirmación de acciones	Se debe solicitar una confirmación al realizar una determinada acción	P20 = V	1
NR-11	Registro de ubicación	Se debe informar si se accedió al sistema desde una ubicación desconocida	P22 = V	1

R-12	Registro de acciones y datos	Se debe poseer un historial de acciones realizadas, o un registro de fecha y hora de ingreso al sistema o de la dirección IP desde la cual se ingresa o del tipo de navegador y sistema de operación utilizado	P17 | P24 | P25 | P26 = V	1
R-13	Control de ubicación	Se debe dar aviso cuando se accede al sistema desde una ubicación desconocida	P22 = V	1
A-14	Comprobación de identidad	El sistema debe realizar una comprobación de identidad mediante alguno de los siguientes métodos: datos biométricos, tarjeta de coordenadas, credenciales, firma electrónica o certificado digital	P27 | P30 | P31 | P32 | P33 = V	1
A-15	Comprobacion es adicionales	Se debe poseer un sistema de verificación en dos pasos, o se debe requerir una clave de segundo nivel para el ingreso al sistema o una confirmación de registro mediante un mail	P28 | P29 | P13 = V	1

3.3 Métricas para cada subcaracterística.

Se combinaron los CE para definir las métricas que satisfacen los objetivos de las subcaracterísticas. Para cada una se definió un nombre, un propósito, un método de aplicación, valores de entradas y formula aplicada.

Confidencialidad.
Métrica: *Confidencialidad*
Propósito: *¿Cuán eficiente es el sistema a la hora de proteger el acceso de datos e información no autorizados, ya sea accidental o deliberadamente?*
Método de aplicación: *Contestar las preguntas de los CE correspondientes a la subcaracterística "Confidencialidad" y calcular la puntuación obtenida, sumando los puntajes de los CE referenciados que cumplan con la meta esperada. "Puntaje total" hace referencia al máximo puntaje que se puede obtener.*
Entradas: *A = Puntaje obtenido. B = Puntaje total.*
Fórmula: *X = A/B*
Observaciones: Los CE a utilizar son: C-1, C-2, C-3 y C-4.

Integridad.
Métrica: *Integridad*
Propósito: *¿Cuán capaz es el sistema a la hora de prevenir accesos o modificaciones no autorizados a datos o programas de ordenador?*
Método de aplicación: *Contestar las preguntas de los CE correspondientes a la sub-característica "Integridad" y calcular la puntuación obtenida, sumando los puntajes de los CE referenciados que cumplan con la meta esperada. "Puntaje total" hace referencia al máximo puntaje que se puede obtener.*

Entradas: *A = Puntaje obtenido. B = Puntaje total.*
Fórmula: *X = A/B*
Observaciones: Los CE a utilizar son: I-5, I-6 e I-7.

No-Repudio.
Métrica: *No-Repudio*
Propósito: *¿Cuán capaz es el sistema de demostrar las acciones o eventos que han tenido lugar, de manera que dichas acciones o eventos no puedan ser repudiados posteriormente?*
Método de aplicación*: Contestar las preguntas de los CE correspondientes a la sub-característica "No-Repudio" y calcular la puntuación obtenida, sumando los puntajes de los CE referenciados que cumplan con la meta esperada. "Puntaje total" hace referencia al máximo puntaje que se puede obtener.*
Entradas*: A = Puntaje obtenido. B = Puntaje total.*
Fórmula: *X = A/B*
Observaciones: Los CE a utilizar son: NR-8, NR-9, NR-10 y NR-11.

Responsabilidad.
Métrica: *Responsabilidad*
Propósito: *¿Cuán capaz es el sistema de rastrear de forma inequívoca las acciones de una entidad?*
Método de aplicación*: Contestar las preguntas de los CE correspondientes a la subcaracterística "Responsabilidad" y calcular la puntuación obtenida, sumando los puntajes de los CE referenciados que cumplan con la meta esperada. "Puntaje total" hace referencia al máximo puntaje que se puede obtener.*
Entradas: *A = Puntaje obtenido. B = Puntaje total.*
Fórmula: *X = A/B*
Observaciones: Los CE a utilizar son: R-12 y R-13.

Autenticidad.
Métrica: *Autenticidad*
Propósito: *¿Cuán capaz es el sistema de demostrar la identidad de un sujeto o un recurso?*
Método de aplicación*: Contestar las preguntas de los CE correspondientes a la subcaracterística "Autenticidad" y calcular la puntuación obtenida, sumando los puntajes de los CE referenciados que cumplan con la meta esperada. "Puntaje total" hace referencia al máximo puntaje que se puede obtener.*
Entradas: *A = Puntaje obtenido. B = Puntaje total.*
Fórmula: *X = A/B*
Observaciones: Los CE a utilizar son: A14 y A15.

Las fórmulas aplicadas para cada subcaracterística se presentan en la Tabla 3.

Tabla 3. Fórmula para cada subcaracterística

MÉTRICA	FÓRMULA
CONFIDENCIALIDAD	(C1+C2+C3+C4)/4
INTEGRIDAD	(I5+I6+I7)/3
NO REPUDIO	(NR8+NR9+NR10+NR11)/4
RESPONSABILIDAD	(R12+R13)/2
AUTENTICIDAD	(A14+A15)/2

4 Casos de Estudio

Se realizó el proceso de evaluación según la estructura de la ISO/IEC 25040 en tres aplicaciones web, con el propósito de evaluar la característica de ***Seguridad***.

Caso a) Se encuentra en producción desde hace aproximadamente 18 meses, posee más de 3200 usuarios, con una frecuencia promedio de 500 accesos diarios.
Caso b) Se encuentra en producción desde hace aproximadamente 30 meses, posee más de 160 usuarios, con una frecuencia promedio de uso de 75 accesos diarios
Caso c) Se encuentra en etapa de testing, posee diez usuarios con una frecuencia mínima por los usuarios que realizan el testing de la aplicación.

4.1 Establecer los requisitos de la evaluación

El propósito de la evaluación es medir, analizando diferentes aspectos, la seguridad de tres sistemas web. En base al propósito se selecciona la característica "***Seguridad***" definida en la norma ISO/IEC 25010.
Dos de los sistemas a evaluar se encuentran en su versión final y están siendo utilizados por diferentes usuarios. El sistema restante se encuentra en una versión de prueba, y está bajo el uso de diferentes personas encargadas del testing.

4.2 Especificar la evaluación

Las métricas para las subcaracterísticas, son las definidas en el apartado 3). Los criterios de aceptación para las subcaracterísticas son:
Inaceptable: 0 <= X < 40
Mínimamente aceptable: 40 <= X < 60
Rango objetivo: 60 <= X < 90
Excede los requerimientos: 90 <= X <=100
El propósito se considerará aceptado si todas las subcaracterísticas se encuentran entre los rangos mínimamente aceptables y excede los requerimientos

4.3 Diseñar la evaluación

Para realizar la evaluación se les solicitó a tres personas encargadas del desarrollo de los sistemas web a evaluar (un desarrollador por cada sistema) que respondieran con V/F las diferentes preguntas planteadas en el apartado 3.1. Además, se les brindó una

planilla de Excel preparada para el ingreso de las respuestas, y en la misma se obtuvieron automáticamente los valores A y B de las métricas.

4.4 Ejecutar la evaluación

Se ejecutó la evaluación según lo planificado y se obtuvieron los siguientes resultados:

Caso a) *Confidencialidad* 88%, *Integridad* 67%, *No-Repudio* 50%, *Responsabilidad* 50% y *Autenticidad* 0%
Caso b) *Confidencialidad* 75%, *Integridad* 100%, *No-Repudio* 75%, *Responsabilidad* 50% y *Autenticidad* 50%
Caso c) *Confidencialidad* 0%, *Integridad* 33%, *No-Repudio* 50%, *Responsabilidad* 0% y *Autenticidad* 0%

4.5 Finalización de la evaluación

El caso a) posee las subcaracterísticas *Confidencialidad* e *Integridad* en el rango aceptable, *No-Repudio* y *Responsabilidad* mínimamente aceptable y *Autenticidad* inaceptable.
El caso b) posee las subcaracterísticas *Integridad* en el rango excede las expectativas, *Confidencialidad* y *No-Repudio* en el rango aceptable, *Responsabilidad* y *Autenticidad* mínimamente aceptable.
El caso c) posee las subcaracterísticas *No-Repudio* en el rango mínimamente aceptable y *Responsabilidad*, *Autenticidad*, *Integridad* y *Confidencialidad* inaceptable.

En la figura 2 se presenta la comparación de las subcaracterísticas evaluadas de cada uno de los casos.

Análisis de la característica – *Seguridad*
El caso a) no cumple con el propósito de la evaluación ya que la subcaracterística *Autenticidad* se encuentra en un rango inaceptable: el sistema no realiza una comprobación de identidad mediante ningún método ni posee un sistema de verificación en dos pasos, una clave de segundo nivel o una confirmación de registro mediante correo electrónico.

El caso b) se considera que cumple con el propósito de la evaluación ya que todas sus subcaracterísticas se encuentran en un rango de aceptación.

El caso c) no cumple con el propósito de la evaluación ya que sólo la subcaracterística *No-repudio* se encuentra en un rango aceptable. La subcaracterística A*utenticidad* es inaceptable por los mismos motivos que en el caso a). En el caso de la *Responsabilidad*, la subcaracterística se considera inaceptable debido a que no se posee un historial de acciones o un registro de acceso, ni tampoco se da aviso cuando

se accede desde una ubicación desconocida. En cuanto a la subcaracterística C*onfidencialidad*, el sistema no posee conexiones seguras ni control de acceso, tampoco se cuenta con una encriptación de los datos de la base de datos ni se establecen criterios para la creación de contraseñas seguras. Por último, la subcaracterística *Integridad*: si bien cuenta con una prevención de modificaciones no autorizadas de la base de datos y del código, no es suficiente para que alcance un nivel de aceptación porque no presenta mecanismos para prevenir el acceso a funcionalidades sin autorización ni realiza confirmaciones de datos vía correo electrónico.

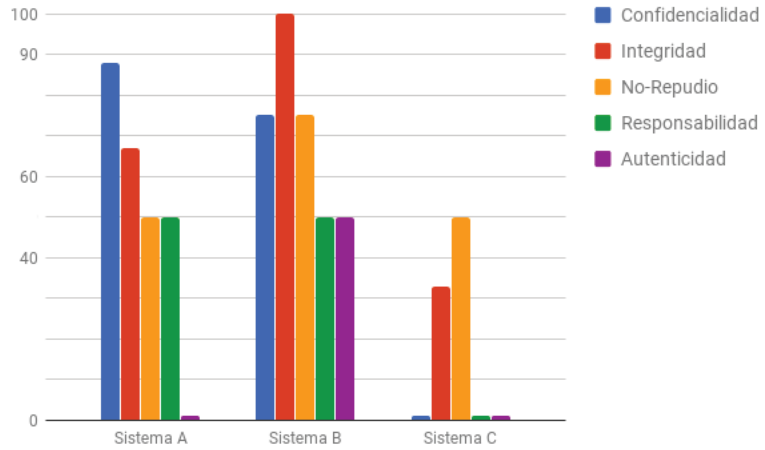

Fig. 1 Subcaracterísticas de cada caso de estudio

5 Conclusiones

La norma ISO/IEC 25010 brinda un modelo de calidad para la evaluación de un conjunto de características aplicables a un producto de software. Se presentó un modelo de evaluación para las características y subcaracterísticas basado en el enfoque GQM, el cual parte de un objetivo concreto para luego crear preguntas asociadas a dicho objetivo, y mediante la combinación de las mismas obtener la métrica en cuestión. Se generaron preguntas para la subcaracterística de la característica ***Seguridad*** y un conjunto de reglas de evaluación para las respuestas a las preguntas, que combinadas generaron las métricas a cada subcaracterística y, en consecuencia, las métricas de la característica.

Se realizó la evaluación en tres sistemas web, donde sólo uno pasó la evaluación de forma positiva. La evaluación del resto de los sistemas fue de mucha utilidad para detectar falencias en los mismos.

Se proyecta ampliar el modelo, generando las preguntas y los criterios de evaluación para las restantes características de la norma ISO/IEC 25010.

6 Referencias

1. S. Esponda, P. Pesado, “Ambiente para la ayuda a la mejora de procesos en las PyMEs”, 2013.
2. ISO, “ISO/IEC 25000:2014 Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Guide to SQuaREtle,” 2014.
3. IRAM and ISO, “IRAM-NM-ISO IEC 9126-1 Information technology. Software engineering. Product quality. Part 1 - Quality model.,” 2009.
4. IRAM;ISO, “IRAM-ISO-IEC 14598-1 Information technology. Software engineering. Software product evaluation. Part 1: General overview,” 2006.
5. V. R. Basili, G. Caldiera, and H. D. Rombach, “The goal question metric approach,” vol. 2, pp. 1–10.
6. ISO, “ISO/IEC 25010:2011 Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- System and software quality models,” 2011.
7. ISO, “ISO/IEC 25040:2011 Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) -- Evaluation process,” 2011.